MS Appeal Brief-Patents
PATENT
4502-1085

# IN THE U.S. PATENT AND TRADEMARK OFFICE BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

| | |
|---|---|
| In re application of | Appeal No. |
| Christopher James MASSAM et al. | Conf. 1633 |
| Application No. 10/540,328 | Group 2456 |
| Filed June 21, 2005 | Examiner Brad McAdams |

NETWORK DEVICE CONFIGURATION

## APPEAL BRIEF

Mail Stop Appeal Brief - Patents
Assistant Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

June 28, 2010

MAY IT PLEASE YOUR HONORS:

## (i) Real Party in Interest

The real party of interest in this appeal is YellowTuna Networks Ltd., Unit 2, 36 William Pickering Drive, Albany, Auckland, New Zealand, 1311

## (ii) Related Appeals and Interferences

None.

## (iii) Status of Claims

Claims 21-32 and 34-39 are pending and stand rejected. Claims 1-20 and 33 were previously cancelled. This appeal is taken from the final rejection of claims 21-32 and 34-39.

## (iv) Status of Amendments

All amendments have been entered.

## (v) **Summary of Claimed Subject Matter**

Independent claim 21 is directed to a method of initializing a network device.

Claim 21 recites a method of providing a VPN communication between two or more network devices (Fig. 1, page 6, lines 21-29) of unknown network address at least a first one of which network devices (page 6, lines 21-29) does not initially know the other network devices internet network addresses (page 6, lines 21-29), the method comprising: providing a verification authority (Fig. 2, 202) connected to the internet (page 6, lines 1-6) remote from the two or more network devices and capable of verifying the identity of the two or more internet network devices (page 5, lines 24-32); providing a configuration server connected to the internet remote from the two or more network devices and capable of supplying to each verified internet device the entire configuration data for that verified internet device (page 6, lines 6-11); providing each of the two or more network devices having no provision to permanently store the user configuration data (page 5, lines 5-13), each of the devices containing configuration information only sufficient to connect the devices to an internet service provider to request a first IP address(page 5, lines 5-13), and using that first IP address to connect to the remote verification authority at a designated internet address (page 5, lines 5-13), providing within each of the two or more network devices(page 5, lines 5-13), a routine which securely contacts the remote verification authority, providing the identity of the network device, and using the designated internet address of that remote verification authority (page 4, line 25 through page 5, line 13), and subsequently downloading from a remote configuration authority authorized by the remote verification authority the entire configuration data each time the device is initialized (page 5, lines 5-13), for one of the two or more internet network devices, each time that device is initialized, reloading that device with the downloaded configuration data (page 5, lines 20-24); and storing the allocated internet network address of the network device at the verification authority (page 6, lines 25 and 26), repeating the process for each of the other network devices so that each of the other network devices downloads from the remote configuration server authorized by the remote verification authority the entire configuration data for that particular internet network device each time that particular device is initialized and reloading that particular device with the downloaded configuration data (page 3, lines 21-27), and storing the allocated internet network address for that particular device at the verification authority (page 6, lines 25 and 26), and initiating a VPN communication between two or more of the network devices (page 6, lines 21-29 ), by sending an instruction (page 6, lines 12-16) from the verification authority to one of the network devices by supplying to that network device the allocated internet address of at least one of the other network devices so that the recipient internet device can communicate with the other network device (page 6, lines 21-29).

Independent claim 28 is directed to a method of initializing a network device.

Claim 28 recites method of providing a VPN communication (Fig. 1, page 6, lines 21-29) over the internet between two or more internet network devices (page 6, lines 21-29) having an allocated or other  internet address at least a first one of which network devices does not initially know the other network devices  internet network addresses (page 6, lines 21-29), the method comprising: providing a remote authority connected to the internet remote from the one or more network devices and capable of verifying the identity of the one or more internet network devices (page 5, line 24-32); and requiring each of the network devices to communicate with the remote authority to inform the remote authority of the current public IP address of the network device(page 6, lines 4 and 5), and storing the current public IP address of each network device at the remote authority (page 6, lines 25 and 26), wherein a VPN can be initiated from the remote authority by sending a request to at least one of the network devices to connect to another of the network devices by sending to the at least one network device the current public IP addresses of the other network devices to which the at least one network device is to be connected(page 6, lines 12-16 and 21-29), wherein each of the two or more network devices does not have any means to permanently store its private configuration data (page 5, lines 5-13) instead is provided with configuration information only sufficient to contact only an internet service provider to request a first IP address (page 5, lines 5-13), and using that first IP address to connect to the remote authority at a designated internet network address of the remote authority (page 5, lines 5-13), and subsequently downloading from a remote configuration service authorized by the remote authority the entire configuration details and software for the specific internet network device each time the device is initialized (page 6, lines 6-11).

## (vi) **Grounds of Rejection to be Reviewed on Appeal**

The first issue on appeal is whether claims 21-29 are obvious, in the meaning of 35 USC § 103(a), based on Hughes, U.S. Patent No. 6,854,009 in view of Remer, U.S. Patent No. 7,120,679 in view of Cochran, U.S. Patent No. 7,240,106.

The second issue on appeal is whether claims 30-32 and 34-39 would have been obvious, in the meaning of 35 USC § 103(a), based on Hughes, U.S. Patent No. 6,854,009 in view of Remer, U.S. Patent No. 7, 120,679 in view of Cochran, U.S. Patent No. 7,240,106 in view of Weldon, U.S. Patent No. 6,366,563.

## (vii) Arguments

**(1) Arguments Concerning the First Ground of Rejection, Claims 21-29 would not have been obvious based on Hughes, Remer and Cochran.**

Hughes discusses a network with multiple servers and multiple distributed client devices each with an operating system. At boot the client connects to one of the servers by whatever means possible and downloads a base operating system and some applications without any user accessible setup. The client may be a thin client, to the extent that there is no hard disk - but there may be flash memory. If there is not, then this ensures that the base operating system must be reloaded each time.

Remer discusses a headless device issuing a configuration request to a configuration service mechanism across network, requesting a configuration specification corresponding to the headless device.

Cochran discusses determining a network address of the computing device.

<u>Claim 21</u>

On page 4 of the Office Action, the Examiner asserts

> However, Hughes does not expressly disclose connecting to a remote verification authority at a designated address, storing the allocated internet network address of the network device at the verification authority and

> supplying said address to at least one of the other network devices.
>
> Remer, in the same field of endeavor, teaches connecting the devices to an internet service provider to request a first IP address, and using that first IP address to connect to the remote verification authority at a designated internet address (**Steps 710-725 and 740, Figure 7; Column 7, Lines 12-40**);

However, claim 21 recites "***each of the devices containing configuration information only sufficient to connect the devices to an internet service provider to request a first IP address***, and using that first IP address to connect to the remote verification authority at a designated internet address … securely contacts the remote verification authority, providing the identity of the network device, and ***using the designated internet address of that remote verification authority.***" (Emphasis added)

Applicants acknowledge that Remer does use an address of a DHCP server to connect to the remote verification authority at a designated internet address (i.e. remote verification authority).

However, it does not do so in the context of being the only address that the headless device can contact. Specifically, Remer, col. 5, lines 59-65 states

> In this case, a DHCP server address may be ***pre-stored in a DHCP server address storage 470*** in the headless device and retrieved whenever a routable address is to be determined. The routable address 490 ***may also be selected from a set of alternative routable addresses pre-stored in an alternative routable address storage 460.*** [Emphasis added]

Thus, Remer may use the address from the DHCP address storage 470 to get an IP address or it may just use a prior routable address pre-stored in an alternative routable address storage 460.

As such, the device of Remer clearly does not limit its self to ***only*** configuration information to contact the remote verification authority to receive a first IP address using the designated internet address of that remote verification authority.

Additionally, Hughes, col. 4, lines 11-36 state

> The very first time a user connects to the system, an ***initial connection is formed over a telephone line or Ethernet connection to a local server*** (discussed in greater detail below) when the client 132, 141a is started up, and may use virtual private network (VPN) tunneling. Preferably, the initial connection provides security by encryption, and on-the-fly compression. (The type of compression may vary depending on the type of files downloaded, and is determined by the server). Compression may be used on any link between the server farm 200 and the client 132, 141, as described below with reference to FIG. 1B. This initial connection may be formed using a reduced version of the operating system (OS), referred to hereinafter as the "boot operating system."
>
> ***Subsequent connections to the network are preferably formed using Internet Protocol (IP) on a high speed communications link, such as an Ethernet coupled to a cable modem, satellite link, or digital subscriber line (DSL)***. These connections may be made with the server farm 100, or with a regional server 122, described below with reference to FIG. 1B. Alternatively, low speed (dial-up) connections may be used for subsequent connections, although performance is not as good with a dial-up connection. Performance using a low-speed dial-up connection may be improved by using an external hard drive for local caching of program files and data, as described below. [Emphasis added]

Thus, as Hughes indicates that it has multiple methods of contacting a remote verification authority. A first time method and subsequent method of contacting the remote verification authority, it seems clear that Hughes does not disclose "each of the devices containing configuration information ***only sufficient to connect the devices to an internet service provider to request a first IP address***, and using that first IP address to connect to the remote verification authority at a designated internet address … ***using the designated internet address of that remote verification authority.***" (Emphasis added)

Further, as quoted above, Hughes states "the client 132, 141a is started up, and may use virtual private network (VPN) tunneling." This makes inherent that Hughes already has some sort of internet connection when it contacts a remote authority. However, the present claim contacts the remote authority as its first action. (i.e. with no existing connection)

Further, as Remer discloses using the designated internet address of that remote verification authority it would teach away from the combining with a DHCP server as in Cochran which responds to a broadcast query.

Further, neither the authentication server 216 of Hughes nor the system of Remer nor the DHCP server of Cochran distribute the network address of the client to a third party. Thus, neither reference discloses "subsequently downloading from a remote configuration authority authorized by the remote verification authority the ***entire*** configuration data each time the device is initialized," (Emphasis added) as in claim 21.

For example, Hughes, col. 8, lines 33-37, state "Only files needed to launch the OS's and applications are initially downloaded; ***additional OS files and/or program files are downloaded later*** when requested (e.g., invoked by the software in the client during execution of a program)." (Emphasis added)

Thus, as additional OS and/or program files are downloaded later, the entire configuration data is not downloaded in Hughes.

Further, Hughes states at col. 8, lines 15-20 states "Because ***only the necessary/frequently used files are transferred*** to RAM (not a disk), and because a high speed (e.g., cable modem or DSL) link 111 is used, ***the time required to boot the client 132, 141a is comparable to the time*** that would be required to boot a system with a locally stored operating system from a hard drive." (Emphasis added)

Thus, Hughes teaches not loading the entire configuration in order to save time. As such, Hughes teaches away from combination with the references that do teach such a feature.

For at least the reasons discussed above, claim 21 and the claims dependent therefrom are not obvious over the combination of Hughes, Remer and Cochran.

Claims 28

Claim 28 recites "wherein each of the two or more network devices does not have any means to permanently store its private configuration data instead is ***provided with configuration information only sufficient to contact only an internet service provider to request a first IP address, and using that first IP address to connect to the remote authority at a designated internet network address of the remote authority.***" (Emphasis added)

Applicants acknowledge that Remer does use an address of a DHCP server to connect to the remote verification authority at a designated internet address (i.e. remote verification authority).

However, it does not do so in the context of being the only address that the headless device can contact. Specifically, Remer, col. 5, lines 59-65, as quoted above, may use the address from the DHCP address storage 470 to get an IP address or it may just use a prior routable address pre-stored in an alternative routable address storage 460.

As such, the device of Remer clearly does not limit its self to ***only*** configuration information to contact the remote verification authority to receive a first IP address using the designated internet address of that remote verification authority.

Additionally, as quoted above Hughes, col. 4, lines 11-36, indicate that it has a method of contacting a remote verification authority a first time and subsequent manner of contacting the remote verification authority, it seems clear that Hughes does not disclose "wherein each of the two or more network devices does not have any means to permanently store its private configuration data instead is ***provided with configuration information only sufficient to contact only an internet service provider to request a first IP address, and using that first IP address to connect to the remote authority at a designated internet network address of the remote authority***." (Emphasis added)

Further, as quoted above, Hughes states "the client 132, 141a is started up, and may use virtual private network (VPN) tunneling." This makes inherent that Hughes already has some sort of internet connection when it contacts a remote authority. However, the present claim contacts the remote authority as its first action. (i.e. with no existing connection)

Further, as Remer discloses using the designated internet address of that remote verification authority it would teach away from the combining with a DHCP server as in Cochran which responds to a broadcast query.

Further, neither the authentication server 216 of Hughes nor the system of Remer nor the DHCP server of Cochran distribute the network address of the client to a third party.

Thus, neither reference discloses “subsequently downloading from a remote configuration service authorized by the remote authority the ***entire*** configuration details and software for the specific internet network device each time the device is initialized,” (Emphasis added) as in claim 28.

For example, Hughes, col. 8, lines 33-37, state “Only files needed to launch the OS's and applications are initially downloaded; ***additional OS files and/or program files are downloaded later*** when requested (e.g., invoked by the software in the client during execution of a program).” (Emphasis added)

Thus, as additional OS and/or program files are downloaded later, the entire configuration data is not downloaded in Hughes.

Further, Hughes states at col. 8, lines 15-20 state “Because ***only the necessary/frequently used files are transferred*** to RAM (not a disk), and because a high speed (e.g., cable modem or DSL) link 111 is used, ***the time required to boot the client 132, 141a is comparable to the time*** that would be required to boot a system with a locally stored operating system from a hard drive.” (Emphasis added)

Thus, Hughes teaches not loading the entire configuration in order to save time. As such, Hughes teaches away from combination with the references that do teach such a feature.

For at least the reasons discussed above, claim 21 and the claims dependent there from are not obvious over the combination of Hughes, Remer and Cochran.

**(2) Arguments Concerning the Second Ground of Rejection, Claims 30-32 and 34-39 would not have been obvious based on Hughes, Remer, Cochran and Weldon.**

Claims 30-32 and 34-39

Claims 30-32 and 34-39 are dependent from otherwise allowable base claims.

Therefore, for at least the reasons discussed above, Hughes, Remer, Cochran and Weldon, taken separately or in combination, fail to render obvious the features of claims 30-32 and 34-39.

## Conclusion

Appellants respectfully urge that the rejections on appeal should not be maintained, and respectfully requests that these rejections be reversed.

The fee for the Appeal Brief in the amount of $540.00 is being paid online herewith by credit card.

If necessary, the Commissioner is hereby authorized in this, concurrent, and future submissions, to charge any underpayment or credit any overpayment to Deposit Account No. 25-0120 for any additional fees required under 37 C.F.R. § 1.16 or under 37 C.F.R. § 1.17.

Respectfully submitted,

YOUNG & THOMPSON

/James J. Livingston, Jr./

James J. Livingston, Jr.
Reg. No. 55,394
209 Madison Street, Suite 500
Alexandria, VA 22314
Telephone (703) 521-2297
Telefax (703) 685-0573
(703) 979-4709

JJL/jlw

June 28, 2010

(viii) Claims Appendix

21. A method of providing a VPN communication between two or more network devices of unknown network address at least a first one of which network devices does not initially know the other network devices internet network addresses, the method comprising:

providing a verification authority connected to the internet remote from the two or more network devices and capable of verifying the identity of the two or more internet network devices;

providing a configuration server connected to the internet remote from the two or more network devices and capable of supplying to each verified internet device the entire configuration data for that verified internet device;

providing each of the two or more network devices having no provision to permanently store the user configuration data, each of the devices containing configuration information only sufficient to connect  the devices to an internet service provider to request a first IP address, and using that first IP address to connect to the remote verification authority at a designated internet address, providing within each of the two or more network devices, a routine which securely contacts the remote verification authority, providing the identity of the network device, and using the designated internet address of that remote verification authority, and subsequently downloading from a remote configuration authority authorized by the remote verification authority the entire configuration data each time the device is initialized, for one of the two or more internet network devices, each time that device is initialized, reloading that device with the downloaded configuration data; and

storing the allocated internet network address of the network device at the verification authority, repeating the process for each of the other network devices so that each of the other network devices downloads from the remote configuration server authorized by the remote verification authority the entire configuration data for that particular internet network device each time that particular device is initialized and reloading that particular device with the downloaded configuration data, and storing the allocated internet network address for that particular device at the verification authority, and initiating a VPN communication between two or more of the network devices, by sending an instruction from the verification authority to one of the network devices by supplying to that network device the allocated internet address of at least one of the other network devices so that the recipient internet device can communicate with the other network device.

22. The method as claimed in claim 22, wherein the two or more network devices are routers.

23. The method as claimed in claim 21, wherein the routers form part of ADSL modems.

24. The method as claimed in claim 21, wherein the configuration data is downloaded as a single transaction.

25. The method as claimed in claim 21, wherein the configuration data is lost when the network device loses power.

26. The method as claimed in claim 24, wherein the configuration data remains unchanged for the duration of the network devices powered on cycle.

27. The method as claimed in claim 24, wherein the configuration data is only downloaded upon a power up sequence.

28. A method of providing a VPN communication over the internet between two or more internet network devices having an allocated or other internet address at least a first one of which network devices does not initially know the other network devices internet network addresses, the method comprising:

providing a remote authority connected to the internet remote from the one or more network devices and capable of verifying the identity of the one or more internet network devices; and

requiring each of the network devices to communicate with the remote authority to inform the remote authority of the current public IP address of the network device, and storing the current public IP address of each network device at the remote authority, wherein a VPN can be initiated from the remote authority by sending a request to at least one of the network devices to connect to another of the network devices by sending to the at least one network device the current public IP addresses of the other network devices to which the at least one network device is to be connected,

wherein each of the two or more network devices does not have any means to permanently store its private configuration data instead is provided with configuration information only sufficient to contact only an internet service provider to request a first IP address, and using that first IP address to connect to the remote authority at a designated internet network address of the remote authority, and subsequently downloading from a remote configuration service authorized by the remote authority the entire configuration details and software for the specific internet network device each time the device is initialized.

29. A method as claimed in claim 28, wherein a user sends a request via secure internet access to the remote authority to create a VPN between some or all of the network devices whose addresses have been stored at the remote authority.

30. A method as claimed in claim 29, wherein each of the two or more network devices communicate with the remote authority on schedule to send statistics for storage and analysis.

31. A method as claimed in claim 30, wherein each of the two or more network devices are routers.

32. A method as claimed in claim 31, wherein the routers form part of ADSL modems.

34. A method as claimed in claim 33, wherein the configuration details and software are downloaded as a single transaction.

35. A method as claimed in claim 34, wherein the configuration details and software are lost when the network device loses power.

36. A method as claimed in claim 35, wherein the configuration details and software remain unchanged for the duration of the network devices “powered on” cycle.

37. A method as claimed in claim 36, wherein the configuration details and software are only downloaded upon a power up sequence.

38. A method as claimed in claim 34, wherein the remote authority sends a code to at least one of the network devices which forces it to download the configuration details and software.

39. A method as claimed in claim 34, wherein the user configuration details and software can be changed by a user via a secure internet connection to the remote authority.

## (ix) **Evidence Appendix**

None.

## (x) Related Proceedings Appendix

None.